

ANTHONY BOUÉ - MAXIME GILLES  
BTS SIO SISR - 1A

# PRÉSENTATION ENTREPRISE



**paloalto**<sup>®</sup>  
**NETWORKS**

# PRÉSENTATION PALO ALTO NETWORKS

## CARACTÉRISTIQUE

Type d'organisation

But

Nature de l'activité

Taille

Ressources :

- Capitalisation boursière

- Effectifs

- Site social

- Immatérielles

- Technologique

- Chiffre d'affaires

- Bénéfice brut

- Champ d'action

- Nationalité

## PALO ALTO

Entreprise privée

Lucratif

Sécurité informatique

Grande entreprise

49,9 milliards de \$

10 473 collaborateurs

Santa Clara, Californie, USA

logo, image de marque

Site Internet, Logo

4, 256 milliards \$

2, 981 milliards \$

Mondial

Etats-Unis (américaine)

# PRINCIPAUX CONCURRENTS

Cisco crée en 1984 est actuellement le leader mondial de matériel réseaux. C'est une entreprise américaine. Son siège social est à San José (Californie). Son effectif est de 75 900 salariés. Sa capitalisation boursière est de 232 milliards \$ pour un chiffre d'affaire de 40 milliards \$. Cisco et Palo Alto Network sont en concurrence sur c'est marché commun : Pare-feu, Cloud Access, réseaux privés virtuels.

Fortinet est une multinationale américaine spécialisée dans la vente de logiciels de Cybersécurité Fortinet. Son siège social est à Sunnyvale (Californie). Son effectif est de 5 845 salariés. Sa capitalisation boursière est de 54, 21 milliards \$.

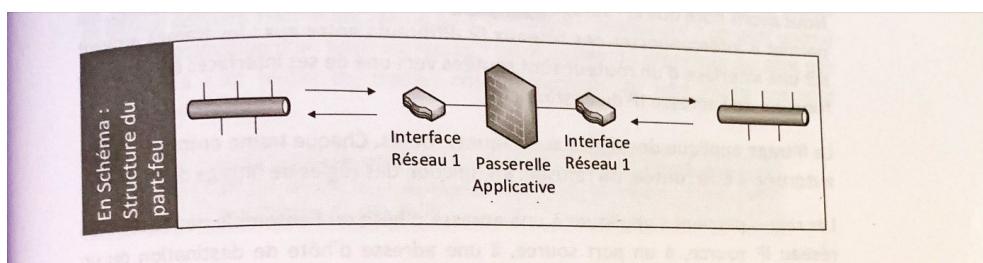
Palo Alto Network sont en concurrence sur les marchés commun : les pare-feu, logiciels de cybersécurité, cloud Access, les mails sécurisés (mail Security).

Ce sont trois entreprises formant un trio de concurrence dans le monde des entreprises de cybersécurité et réseaux.

# PRÉSENTATION DE LA NOTION DE PARE-FEU :

Un pare-feu ou pont de barrière est un pont particulier permettant de mettre en place de la sécurité entre deux réseaux (de norme identique ou non). Il peut également être utilisé pour gérer les transferts de données entre des sous-réseaux logiques.

Selon les objectifs souhaités, le filtrage appliqué au niveau de la passerelle applicatif portera sur :



- L'adressage des hôtes,
- Les protocoles de niveau application,
- Le contenu des données.

Un pare-feu est un routeur sécurisé interposé entre Internet et votre réseau. Sa seule tâche est de filtrer et tout ce qui entre et sort. C'est une sorte de vigile entre Internet et le réseau. Tout le trafic transite par le pare-feu qui autorise ou interdit les accès.

Un pare-feu est absolument obligatoire dès lorsque votre réseau accède à Internet, que ce soit par une connexion à haut débit, ligne T1, ou tout autre connexion haut débit. Sans pare-feu, les pirates découvriront tôt ou tard l'existence de votre réseau non protégé, le signaleront alors à leurs collègues et il en subira les conséquences en quelques heures.

Un pare-feu peut être installé de deux manières. La plus simple consiste à acheter un équipement par feu, qui était aurait été un écouteur offrant des fonds ça a été de pare-feu. La plupart sont équipés d'une interface de type Web permettant de les connecter directement depuis l'un des ordinateurs du réseau à l'aide d'un navigateur. Vous les configurez ensuite selon vos besoins.

# PRÉSENTATION DU PARE-FEU PALO ALTO NETWORK :

Dans la présentation du pare-feu nouvelle génération de Palo Alto, nous pouvons accéder à toutes les données essentielles du pare-feu via un fenêtre clair avec différentes catégories. Dans ce tableau de bord, nous pouvons accéder aux informations générales, notamment les versions, l'adresse IP, le masque de sous-réseau, et aussi le nom de la machine et le type de licence qu'on a. Nous avons la possibilité, à percevoir les personnes qui se sont connectées en administrateur, à percevoir les différentes adresses IP. Depuis un logiciel ou depuis un site web, la date et l'heure de fin et de début de session. Assurer que tout fonctionne. En survolant les différentes catégories de la fenêtre du pare-feu, il est capable d'analysés l'activité du réseau, les différents sites Internet qui ont été visités sur le réseau, classé suivant les sessions les tâches, le contenu, les utilisateurs, les profils, ainsi que la source et la destination des connexions suivant les pays.

Le pare-feu classe tout le trafic. Tout le trafic est classifié indépendamment du port, du chiffrement (SSL ou SSH) ou de la technique d'évasion. Les applications non identifiées qui ne représentent qu'un faible pourcentage du trafic, mais qui constitue un risque potentiellement élevé, sont automatiquement classifiée et font l'objet d'une gestion systématique.

Le pare-feu est capable de réduire les menaces en autorisant certaines applications et en refusant toutes les autres. Grâce à une base de données, il peut détecter les malwares et les menaces inconnues. Elles sont analysées et classifiées, le pare-feu attribue automatiquement une signature du fichier infecté et du trafic et nous avertit.

Le pare-feu de Palo Alto Networks a l'avantage de pouvoir s'installer sur des machines physiques (smartphone, ordinateur portable et de bureau, serveur), des appareils virtuel (machine VMware) ou des services cloud (azure, aws) et qui sont gérés exactement de la même manière.

Il est possible d'afficher la cartographie des applications dans un format claire et lisible. Ajouter et supprimer des filtres pour en savoir plus sur l'application, ses fonctions et leurs utilisateurs. Grâce à Wildfire, une analyse est faite à la recherche des malwares qui sont enregistrés et leurs détails sont pleinement accessible comme par exemple l'application utiliser l'utilisateur le type de fichiers.

# SUITE :

Un éditeur de politique de sécurité unifié permet de créer et de déployer rapidement des règles qui contrôlent les applications, les groupes d'utilisateurs et les contenus. Comme par exemple appliquer des règles sur la navigation Internet pour tous les utilisateurs en autorisant et analysant le trafic vers des sites Web liés aux activités de l'entreprise ou bloqué ou encadrer l'accès au site sans rapport. Et dans ce cas-là appliquer des actions, comme par exemple intervention d'un antivirus qui bloque les menaces, d'un anti-spyware qui détecte analyse et stoppe les malwares. WildFire peut intervenir en cas de menaces inconnue en appliquant une analyse du comportement du fichier inconnu dans différents systèmes d'exploitation.

Pour conclure :

- Nous pouvons optimiser notre politique de sécurité en remplaçant les règles traditionnelles par des règles passées sur les applications et l'utilisation.
- Évaluation des meilleures pratiques et passer en revue le cycle de vie de la sécurité. C'est-à-dire évaluer notre niveau à prévenir un risque en cas de menace.
- Les principales fonctionnalités du pare-feu de Palo Alto sont la prévention d'intrusion, l'analyse de malware, la protection contre les pertes de données, la sécurité à l'accès au cloud, prévention

3 questions relatives au parcours professionnel :

- Quelle étude avez-vous fait pour en arriver là ? En alternance ou pas ?
- Dans quelle entreprise était-il avant ?
- Quelle perspective d'évolution dans le futur ?

3 questions sur les aspects techniques en lien avec les produits de Palo Alto Network :

- Votre nouvelle génération de pare-feu permet-elle d'être aux normes avec les réglementations sur la vie privée et la protection des données ? N'avez-vous pas peur d'avoir l'impression de pister vos salariés ?
- Vos solutions de sécurité sont-elles capables de faire face à tous les types d'attaques et de menaces notamment les ransomwares qui passe par la mémoire vidéo d'une carte graphique ?